

Private Broadcasting over Independent Parallel Channels

Ashish Khisti *Member, IEEE*, and Tie Liu *Member, IEEE*

Abstract

We study private broadcasting of two messages to two groups of receivers over independent parallel channels. One group consists of an arbitrary number of receivers interested in a common message, whereas the other group has only one receiver. Each message must be kept confidential from the receiver(s) in the other group. Each of the sub-channels is degraded, but the order of receivers on each channel can be different. While corner points of the capacity region were characterized in earlier works, we establish the capacity region and show the optimality of a superposition strategy. For the case of parallel Gaussian channels, we show that a Gaussian input distribution is optimal. We also discuss an extension of our setup to broadcasting over a block-fading channel and demonstrate significant performance gains using the proposed scheme over a baseline time-sharing scheme.

I. INTRODUCTION

There has been a considerable amount of interest in recent years in exploiting the properties of fading wireless channels for transmission of confidential messages (see e.g., [1]–[6] and references therein). Such studies have lead to new coding techniques such as the variable rate extension of the wiretap codebook [1], secure product codebooks [7] and secure multicast codebooks [4]. In the present work we study a setup where a single transmitter needs to serve two groups of receivers over a block-fading channel. There are K receivers in group 1, all interested in a common message, whereas there is a single receiver in group 2. The message of group 1 must be kept confidential from the group 2 receiver, whereas the message of group 2 must be kept confidential from group 1. We will refer to this setup as *private broadcasting*. In related work, references [8]–[10] study private broadcasting when there is one receiver in each group. References [11], [12] study private broadcasting with feedback over erasure and MIMO broadcast channels. Reference [13] studies interference alignment techniques

A. Khisti is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: akhisti@comm.utoronto.ca). T. Liu is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA (e-mail: tieliu@tamu.edu).

A. Khisti's work was supported by an NSERC (Natural Sciences Engineering Research Council) Discovery Grant and an Ontario Early Researcher Award. T. Liu was supported by the National Science Foundation under Grants CCF-08-45848 and CCF-09-16867.

Part of this work was presented in the IEEE International Symposium on Information Theory (ISIT), Cambridge, MA, July, 2012

for private broadcasting. In this paper we focus on the case when there are M independent, parallel and degraded sub-channels and thereafter treat the natural extension to block-fading channels.

Our setup reduces to previously known results at the corner points of the capacity region. When we only need to transmit the message for group 1, with the group 2 receiver as the only eavesdropper, the capacity can be achieved using a secure multicast codebook [4]. Instead, when we only need to transmit the message for group 2, with all receivers in group 1 as eavesdroppers, the capacity can be achieved using a secure product codebook [7]. Interestingly the secure multicast and secure product codebook constructions are based on different ideas. A secure multicast codebook consists of M sub-codebooks, one for each channel. Each sub-codebook is a wiretap codebook [14], has the same rate as the transmitted message and guarantees confidentiality of the message from the eavesdropper on its respective link. The secure multicast construction guarantees that the legitimate receiver can decode the message by using the output of all the channels. Furthermore the message remains confidential from the eavesdropper even when all the channel outputs are combined. While the secure product codebook also uses one sub-codebook for each sub-channel, the rate of each sub-codebook equals the capacity of the legitimate receiver on that sub-channel. The secure product codebook takes a cartesian product of these codebooks and then applies the wiretap construction to this product codebook. This guarantees that the output codeword on any given sub-channel is (nearly) independent of the output codewords on other sub-channels. This limits the amount of information that gets leaked to an eavesdropper on any given sub-channel. Both the secure multicast codebook and secure product codebook result in a higher rate than a vector extension of the wiretap codebook to parallel channels.

In this paper we study the case when both the messages need to be simultaneously transmitted. We find that a superposition construction achieves the entire capacity region. The proposed construction imposes a particular layering order for the secure multicast and secure product codebooks. The codewords in each sub-codebook of the secure product codebook must constitute the cloud centers, whereas the codewords in the associated sub-codebook of the secure multicast codebook must constitute satellite codewords. The optimality of such a layered coding scheme was somewhat unexpected. In absence of secrecy constraints, to the best of our knowledge the capacity region in the proposed setup remains open, even though the corner points are known [15]. We will provide an explanation on the sufficiency of the superposition approach after presenting the coding scheme in section III.

For the case of independent Gaussian sub-channels, we further establish that a Gaussian input distribution is optimal. The proof involves obtaining a Lagrangian dual for every boundary point of the capacity region and then using an extremal inequality [16], [17] to show that the expression is maximized using Gaussian inputs. The result for the Gaussian channels are extended to a block-fading channel model using suitable quantization of the channel gains. We numerically evaluate the rate region for a sub-optimal power allocation and observe significant gains over a naive time-sharing approach.

II. PROBLEM STATEMENT AND MAIN RESULTS

A. Independent Parallel Channels

Our setup involves M independent parallel sub-channels and two groups of receivers. There are K receivers in group 1 and one receiver in group 2. The output symbols at receiver k in group 1 across the M sub-channels is denoted by

$$\mathbf{y}_k = (y_{k,1}, y_{k,2}, \dots, y_{k,M}), \quad k = 1, 2, \dots, K, \quad (1)$$

whereas the output symbols of the group 2 receiver across the M sub-channels are denoted by

$$\mathbf{z} = (z_1, z_2, \dots, z_M), \quad (2)$$

and the channel input symbols are denoted by $\mathbf{x} = (x_1, \dots, x_M)$.

Each sub-channel is a degraded broadcast channel. The degradation on sub-channel i can be expressed as

$$x_i \rightarrow y_{\pi_i(1),i} \cdots y_{\pi_i(l_i),i} \rightarrow z_i \rightarrow y_{\pi_i(l_i+1),i} \cdots y_{\pi_i(K),i}, \quad (3)$$

for some permutation $\{\pi_i(1), \dots, \pi_i(K)\}$ of the set $\{1, \dots, K\}$.

We intend to transmit message m_1 to receivers $1, \dots, K$ in group 1, while the message m_2 must be transmitted to the receiver in group 2. A length- n private broadcast code encodes a message pair $(m_1, m_2) \in [1, 2^{nR_1}] \times [1, 2^{nR_2}]$ into a sequence \mathbf{x}^n such that $\Pr(m_1 \neq \hat{m}_{1,k}) \leq \varepsilon_n$, and $\Pr(m_2 \neq \hat{m}_2) \leq \varepsilon_n$, and furthermore the secrecy constraints

$$\frac{1}{n} I(m_1; \mathbf{z}^n) \leq \varepsilon_n, \quad \frac{1}{n} I(m_2; \mathbf{y}_k^n) \leq \varepsilon_n, \quad k = 1, 2, \dots, K, \quad (4)$$

are also satisfied. Here $\{\varepsilon_n\}$ approaches zero as $n \rightarrow \infty$. The capacity region consists of the set of all rate pairs (R_1, R_2) achieved by some private broadcast code. The following Theorem characterizes this region.

Theorem 1: Let auxiliary variables $\{u_i\}_{1 \leq i \leq M}$ satisfy the Markov condition

$$u_i \rightarrow x_i \rightarrow y_{\pi_i(1),i} \cdots y_{\pi_i(l_i),i} \rightarrow z_i \rightarrow y_{\pi_i(l_i+1),i} \cdots y_{\pi_i(K),i}. \quad (5)$$

The capacity region is given by the union of all rate pairs (R_1, R_2) that satisfy the following constraints:

$$R_1 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^M I(x_i; y_{k,i} | u_i, z_i) \right\} \quad (6)$$

$$R_2 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^M I(u_i; z_i | y_{k,i}) \right\} \quad (7)$$

for some choice of $\{u_i\}_{1 \leq i \leq M}$ that satisfy (5). The alphabet of u_i satisfies the cardinality constraint $|\mathcal{U}_i| \leq |\mathcal{X}_i| + 2K - 1$. \square

The coding theorem and converse for Theorem 1 are presented in section III and IV respectively.

B. Gaussian Channels

Consider the discrete-time real Gaussian model where the channel output over sub-channel i at time index t is given by

$$y_{k,i}(t) = x_i(t) + n_{k,i}(t) \quad (8)$$

$$z_i(t) = x_i(t) + w_i(t), \quad t = 1, \dots, T. \quad (9)$$

The additive noise vectors $\mathbf{n}_{k,i} = (n_{k,i}(1), \dots, n_{k,i}(T))$ and $\mathbf{w}_i = (w_i(1), \dots, w_i(T))$ have entries that are sampled i.i.d. $\mathcal{N}(0, \sigma_{k,i}^2)$ and $\mathcal{N}(0, \delta_i^2)$, respectively. Since the capacity region of the channel depends on the joint distribution of the additive noise $(n_{1,i}(t), \dots, n_{K,i}(t), w_i(t))$ only through the marginals and that Gaussian variables are infinitely divisible, without loss of generality we may assume that for each sub-channel i the receivers are degraded as expressed in (3). We shall consider both the per sub-channel average power constraint

$$\frac{1}{T} E [\|\mathbf{x}_i\|^2] \leq P_i, \quad \forall i = 1, \dots, M \quad (10)$$

and the total average power constraint

$$\frac{1}{T} \sum_{i=1}^M E [\|\mathbf{x}_i\|^2] \leq P \quad (11)$$

where $\mathbf{x}_i = (x_i(1), \dots, x_i(T))$ is the input vector for sub-channel i .

Theorem 2: The capacity region under the per sub-channel average power constraint (10) is given by the union of all rate pairs (R_1, R_2) that satisfy the following constraints:

$$R_1 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^M A_{k,i}^{(1)}(\mathbf{Q}) \right\} \quad (12)$$

$$R_2 \leq \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^M A_{k,i}^{(2)}(\mathbf{Q}) \right\} \quad (13)$$

for some power vector $\mathbf{Q} = (Q_1, \dots, Q_M)$, where $0 \leq Q_i \leq P_i$ for all $i = 1, \dots, M$,

$$A_{k,i}^{(1)}(\mathbf{Q}) := \left[\frac{1}{2} \log \left(\frac{Q_i + \sigma_{k,i}^2}{\sigma_{k,i}^2} \right) - \frac{1}{2} \log \left(\frac{Q_i + \delta_i^2}{\delta_i^2} \right) \right]^+ \quad (14)$$

$$A_{k,i}^{(2)}(\mathbf{Q}) := \left[\frac{1}{2} \log \left(\frac{P_i + \delta_i^2}{Q_i + \delta_i^2} \right) - \frac{1}{2} \log \left(\frac{P_i + \sigma_{k,i}^2}{Q_i + \sigma_{k,i}^2} \right) \right]^+ \quad (15)$$

and $x^+ := \max\{x, 0\}$. □

A proof of Theorem 2 is provided in section V.

Corollary 1: The capacity region under the total average power constraint (11) is given by the union of all rate pairs (R_1, R_2) that satisfy the constraints (12) and (13) for some power vectors $\mathbf{P} = (P_1, \dots, P_M)$ and $\mathbf{Q} = (Q_1, \dots, Q_M)$, where $0 \leq Q_i \leq P_i$ for all $i = 1, \dots, M$ and $\sum_{i=1}^M P_i \leq P$. □

The above corollary follows directly from Theorem 2 and the well-known connection between the per sub-channel and the total average power constraints. We will not provide a proof of Corollary 1.

C. Fading Channels

We consider a block-fading channel model with a coherence period of T complex symbols. The channel output in coherence block i is given by

$$\mathbf{y}_k(i) = h_k(i)\mathbf{x}(i) + \mathbf{n}_k(i) \quad (16)$$

$$\mathbf{z}(i) = g(i)\mathbf{x}(i) + \mathbf{w}(i), \quad i = 1, 2, \dots, M \quad (17)$$

where the channel gains $h_k(i)$ of the K receivers in group 1 and the channel gain $g(i)$ of the group 2 receiver are sampled independently in each coherence block i and stay constant throughout the block. The coherence period T will be taken to be sufficiently large so that random coding arguments can be invoked in each coherence block. The channel input $\mathbf{x}(i) \in \mathbb{C}^T$ satisfies a long-term average power constraint

$$E \left[\frac{1}{MT} \sum_{i=1}^M \|\mathbf{x}(i)\|^2 \right] \leq P \quad (18)$$

whereas the additive noise vectors $\mathbf{n}_k(i)$ and $\mathbf{w}(i)$ have entries that are sampled i.i.d. $\mathcal{CN}(0, 1)$. We are interested in the ergodic communication scenario where the number of blocks M used for communication can be arbitrarily large. Furthermore we assume that the channel gains in each coherence block are revealed to all terminals including the transmitter at the beginning of each coherence block.

Theorem 3: The private broadcasting capacity region for the fading channel model consists of all rate pairs (R_1, R_2) that satisfy the following constraints:

$$R_1 \leq \min_{1 \leq k \leq K} E \left[\left\{ \log \left(\frac{1 + Q(\mathbf{h}, g)|h_k|^2}{1 + Q(\mathbf{h}, g)|g|^2} \right) \right\}^+ \right], \quad (19)$$

$$R_2 \leq \min_{1 \leq k \leq K} E \left[\left\{ \log \left(\frac{1 + P(\mathbf{h}, g)|g|^2}{1 + Q(\mathbf{h}, g)|g|^2} \right) - \log \left(\frac{1 + P(\mathbf{h}, g)|h_k|^2}{1 + Q(\mathbf{h}, g)|h_k|^2} \right) \right\}^+ \right], \quad (20)$$

for some power allocation functions $P(\mathbf{h}, g)$ and $Q(\mathbf{h}, g)$ that satisfy $0 \leq Q(\mathbf{h}, g) \leq P(\mathbf{h}, g)$ for all $(\mathbf{h}, g) \in \mathbb{C}^{K+1}$, and $E[P(\mathbf{h}, g)] \leq P$, where $\mathbf{h} := (h_1, \dots, h_K)$ denotes the channel gains of the receivers in group 1. \square

A proof of Theorem 3 is provided in Section VI.

Theorems 1, 2 and 3 constitute the main results in this paper.

III. CODING THEOREM

The basic idea behind our coding scheme is illustrated in Fig. 1. The message m_2 is encoded using a product codebook [1], [7], whose codewords are obtained by taking cartesian product of the M codebooks, one for each of the parallel channels. The message m_1 is encoded using a multicast codebook [4], also consisting of M codebooks. As shown in Fig. 1, the codewords of the product-codebook constitute cloud centers of the superposition codebook, whereas the codewords of the multicast codebook constitute the satellite codewords. We describe the details of our construction in the following sub-sections.

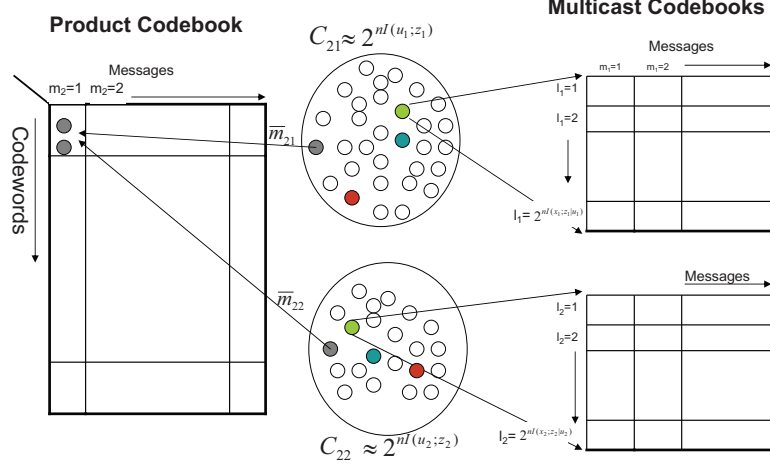


Fig. 1: Superposition construction for the case of two channels. The product codebook for the group 2 user is obtained by taking a cartesian $C_{21} \times C_{22}$ of two independently generated codebooks and binning the resulting codeword pairs. The multicast codebook is generated, conditioned on the codewords of C_{21} and C_{22} .

A. Product-Codebook Construction

The message m_2 is encoded using a product codebook [1], [7]. Let $\mathcal{M}_{2,i}$ be the set of all binary sequences of length $N_{2,i} = n(I(u_i; z_i) - 2\varepsilon)$ i.e.,

$$\mathcal{M}_{2,i} := \{0, 1\}^{N_{2,i}}. \quad (21)$$

On channel i , we generate a codebook $\mathcal{C}_{2,i} : \mathcal{M}_{2,i} \rightarrow \mathcal{U}_i^n$ consisting of $|\mathcal{M}_{2,i}|$ codewords, i.e.,

$$\mathcal{C}_{2,i} := \{u_i^n(\bar{m}_{2,i}) : \bar{m}_{2,i} \in [1, 2^{N_{2,i}}]\}, \quad (22)$$

where each sequence u_i^n is sampled i.i.d. from the distribution $p_{u_i}(\cdot)$. Let

$$\mathcal{M}_2 := \mathcal{M}_{2,1} \times \mathcal{M}_{2,2} \times \dots \times \mathcal{M}_{2,M} \quad (23)$$

$$= \{(\bar{m}_{2,1}, \dots, \bar{m}_{2,M}) : \bar{m}_{2,i} \in \{0, 1\}^{N_{2,i}}, i = 1, \dots, M\}. \quad (24)$$

As shown in Fig. 1, we partition the set \mathcal{M}_2 into 2^{nR_2} bins such that there are $L_2 = 2^{n\{\sum_{i=1}^M I(u_i; z_i) - R_2 - M\varepsilon\}}$ sequences in each bin. Each bin corresponds to one message $m_2 \in [1, 2^{nR_2}]$. Thus given a message m_2 the encoder selects one sequence $(\bar{m}_{2,1}, \dots, \bar{m}_{2,M}) \in \mathcal{M}_2$ uniformly at random from the corresponding bin. On channel i we select the codeword $u_i^n \in \mathcal{C}_{2,i}$ associated with $\bar{m}_{2,i}$. We note that from our construction, each

sequence in \mathcal{M}_2 is equally likely i.e.,

$$\Pr(\bar{m}_{2,1} = \bar{m}_{2,1}, \dots, \bar{m}_{2,M} = \bar{m}_{2,M}) = \prod_{j=1}^M \Pr(\bar{m}_{2,j} = \bar{m}_{2,j}) = \frac{1}{|\mathcal{M}_{2,1}| \times |\mathcal{M}_{2,2}| \dots |\mathcal{M}_{2,M}|}. \quad (25)$$

B. Multicast-Code Construction

The codebook associated with m_1 is a secure multicast codebook [4]. For each $u_i^n \in \mathcal{C}_{2,i}$, and each $m_1 \in [1, 2^{nR_1}]$ we construct a codebook $\mathcal{C}_{1,i}(u_i^n, m_1)$ consisting of a total of $L_{1,i} = 2^{n(I(x_i; z_i | u_i) + \varepsilon)}$ codeword sequences of length n , each sampled i.i.d. from the distribution $\prod_{j=1}^n p_{x_i | u_i}(x_{ij} | u_{ij})$.

Let $l_{1,i}$ be uniformly distributed over $[1, L_{1,i}]$. Given a message $m_1 \in [1, 2^{nR_1}]$ and codewords (u_1^n, \dots, u_M^n) , selected in the base layer, we select the sequence x_i^n from the codebook $\mathcal{C}_{1,i}(u_i^n, m_1)$ corresponding to the randomly and uniformly generated index $l_{1,i}$. The sequence x_i^n is transmitted on sub-channel i .

The following property will be useful in our subsequent analysis.

Lemma 1: The sequences $(x_1^n, x_2^n, \dots, x_M^n)$ are conditionally independent given m_1 .

Proof: Note that

$$p(x_1^n, \dots, x_M^n | m_1) = \sum_{\{\bar{m}_{2,i}\}} p(x_1^n, \dots, x_M^n, \bar{m}_{2,1}, \dots, \bar{m}_{2,M} | m_1) \quad (26)$$

$$= \sum_{\{\bar{m}_{2,i}\}} p(x_1^n, \dots, x_M^n | m_1, \bar{m}_{2,1}, \dots, \bar{m}_{2,M}) p(\bar{m}_{2,1}, \dots, \bar{m}_{2,M}) \quad (27)$$

$$= \sum_{\{\bar{m}_{2,i}\}} p(x_1^n, \dots, x_M^n | m_1, \bar{m}_{2,1}, \dots, \bar{m}_{2,M}) p(\bar{m}_{2,1}) \dots p(\bar{m}_{2,M}) \quad (28)$$

$$= \sum_{\{\bar{m}_{2,i}\}} p(x_1^n | m_1, \bar{m}_{2,1}) \dots p(x_M^n | m_1, \bar{m}_{2,M}) p(\bar{m}_{2,1}) \dots p(\bar{m}_{2,M}) \quad (29)$$

$$= \prod_{i=1}^M \sum_{\bar{m}_{2,i}} p(x_i^n | m_1, \bar{m}_{2,i}) p(\bar{m}_{2,i}) \quad (30)$$

$$= \prod_{i=1}^M \sum_{\bar{m}_{2,i}} p(x_i^n, \bar{m}_{2,i} | m_1) \quad (31)$$

$$= \prod_{i=1}^M p(x_i^n | m_1) \quad (32)$$

where (27) follows from the fact that the messages $\bar{m}_{2,1}, \dots, \bar{m}_{2,M}$ are independent of m_1 ; (28) follows from the fact that the messages satisfy (25); (29) follows from the fact that each $x_i^n \in \mathcal{C}_{1,i}(m_1, u_i^n)$ and u_i^n is a function of $\bar{m}_{2,i}$. Eq. (32) establishes the conditional independence of the messages and completes the proof. \blacksquare

C. Decoding and Error Analysis

1) *Decoding of Message m_1* : Receiver k in group 1 selects those sub-channels \mathcal{J}_k where it is stronger than the group 2 receiver:

$$\mathcal{J}_k = \left\{ i \in [1, M] : x_i \rightarrow y_{k,i} \rightarrow z_i \right\} \quad (33)$$

- For each $i \in \mathcal{J}_k$, receiver k selects a sequence $\hat{u}_i^n \in \mathcal{C}_{2,i}$ such that¹ $(\hat{u}_i^n, y_{k,i}^n) \in T_\varepsilon^n(u_i, y_{k,i})$. We define \mathcal{E}_k as the event that there exists some $i \in \mathcal{J}_k$ such that $\{\hat{u}_i^n \neq u_i^n\}$.
- Receiver k then searches for a message $\hat{m}_1 \in [1, 2^{nR_1}]$ with the following property: for each $i \in \mathcal{J}_k$ there exists a codeword $x_i^n \in \mathcal{C}_{1,i}(m_1, \hat{u}_i^n)$ such that $(x_i^n, y_{k,i}^n) \in T_\varepsilon^n(x_i, y_{k,i}|u_i)$. An error is declared if $\hat{m}_1 \neq m_1$.

Now observe that

$$\Pr(\hat{m}_1 \neq m_1) \leq \Pr(\mathcal{E}_k) + \Pr(\hat{m}_1 \neq m_1 | \mathcal{E}_k^c). \quad (34)$$

Since $|\mathcal{C}_{2,i}| \leq 2^{n(I(u_i; z_i) - \varepsilon)}$ and $I(u_i; y_{k,i}) \geq I(u_i; z_i)$ for each $i \in \mathcal{J}_k$, it follows that $\Pr(\mathcal{E}_k) \leq M\varepsilon$.

To bound the second term in (34) we use the union bound and analysis of typical events.

$$\Pr(\hat{m}_1 \neq m_1 | \mathcal{E}_k^c) \leq 2^{nR_1} \prod_{i \in \mathcal{J}_k} \left\{ |\mathcal{C}_{1,i}| 2^{-n(I(x_i; y_{k,i}|u_i) - \varepsilon)} \right\} \quad (35)$$

$$\leq 2^{nR_1} 2^{-n \sum_{i \in \mathcal{J}_k} (I(x_i; y_{k,i}|u_i) - I(x_i; z_i|u_i) - 2\varepsilon)} \quad (36)$$

$$= 2^{nR_1} 2^{-n \sum_{i \in \mathcal{J}_k} (I(x_i; y_{k,i}|u_i, z_i) - 2\varepsilon)} \quad (37)$$

which goes to zero provided that $R_1 \leq \sum_{i \in \mathcal{J}_k} I(x_i; y_{k,i}|u_i, z_i) - (2M+1)\varepsilon$. Since $\varepsilon > 0$ is arbitrary, our choice of R_1 in (6) thus guarantees that the error probability associated with message m_1 vanishes to zero.

2) *Decoding of message m_2* : The receiver in group 2 decodes message $\bar{m}_{2,i}$ on sub-channel i by searching for a sequence $u_i^n \in \mathcal{C}_{2,i}$ that is jointly typical with z_i^n . Since the number of codewords in $\mathcal{C}_{2,i}$ does not exceed $2^{n(I(u_i; z_i) - 2\varepsilon)}$, this event succeeds with high probability. Hence the receiver correctly decodes $(\bar{m}_{2,1}, \dots, \bar{m}_{2,M})$ and in turn message m_2 with high probability.

D. Secrecy Analysis

In order to establish the secrecy of message m_1 we need to show that

$$\frac{1}{n} I(m_1; \mathbf{z}^n | \mathcal{C}) \leq \varepsilon_n \quad (38)$$

Using Lemma 1 and the fact that the channels are independent, we have that z_1^n, \dots, z_M^n are conditionally independent given m_1 . It follows that

$$\frac{1}{n} I(m_1; \mathbf{z}^n | \mathcal{C}) \leq \sum_{i=1}^M I(m_1; z_i^n | \mathcal{C}). \quad (39)$$

¹We will use the notion of strong typicality. The set $T_\varepsilon^n(x, y)$ denotes the ε -strongly typical set.

Since in our conditional codebook construction, there are $2^{n(I(x_i; z_i | u_i) + \varepsilon)}$ sequences in each codebook $\mathcal{C}_{1,i}(u_i^n, m_1)$, it follows from standard arguments that $\frac{1}{n}I(m_1; z_i^n | \mathcal{C}) \leq \varepsilon_n$. The secrecy constraint (38) now follows.

To establish secrecy of message m_2 with respect to user 1 in group 1, we show that

$$\frac{1}{n}H(m_2 | \mathbf{y}_1^n, m_1) \geq R_2 - \varepsilon_n. \quad (40)$$

where for simplicity we drop the subscript associated with user 1 in the sequence \mathbf{y}_1^n . Without loss of generality, we assume that sub-channels $i = 1, 2, \dots, L$ satisfy $x_i \rightarrow z_i \rightarrow y_i$ while sub-channels $i = L+1, \dots, M$ satisfy $x_i \rightarrow y_i \rightarrow z_i$. Now consider

$$H(m_2 | \mathbf{y}_1^n, m_1) = H(m_2 | y_1^n, \dots, y_M^n, m_1) \quad (41)$$

$$= H(\bar{m}_{2,1}^M | y_1^n, \dots, y_M^n, m_1) - H(\bar{m}_{2,1}^M | m_2, m_1, y_1^n, \dots, y_M^n) \quad (42)$$

$$= \sum_{j=1}^M H(\bar{m}_{2,j} | y_j^n, m_1) - H(\bar{m}_{2,1}^M | m_2, m_1, y_1^n, \dots, y_M^n) \quad (43)$$

$$\geq \sum_{j=1}^L H(\bar{m}_{2,j} | y_j^n, m_1) - H(\bar{m}_{2,1}^M | m_2, m_1, y_1^n, \dots, y_M^n) \quad (44)$$

where (43) follows by establishing that the collection of pairs $\{(m_{2,1}, y_1^n), \dots, (m_{2,M}, y_M^n)\}$ is conditionally independent given m_1 , which can be established in a manner similar to the proof of Lemma 1 and (44) follows from the fact that the entropy function is non-negative and therefore we can drop the terms $L+1, \dots, M$ in the first summation.

We lower bound the first term in (44). Recall that $\bar{m}_{2,j}$ is uniformly distributed over $\mathcal{C}_{2,j}$ with $|\mathcal{C}_{2,j}| = 2^{n(I(u_j; z_j) - \varepsilon)}$. Furthermore, the corresponding codeword u_j^n is the base codeword in $\mathcal{C}_{1,j}(m_1, u_j^n)$ and

$$|\mathcal{C}_{1,j}(m_1, u_j^n)| = 2^{n(I(x_j; z_j | u_j) - \varepsilon)} \geq 2^{n(I(x_j; y_j | u_j) - \varepsilon)},$$

since the channel satisfies the relation $x_j \rightarrow z_j \rightarrow y_j$ for $j = 1, \dots, L$. Since the satellite codeword x_j^n is uniformly selected from $\mathcal{C}_{1,j}$ it follows that [18, Remark 22.2, pp. 554-555]

$$\frac{1}{n}H(\bar{m}_{2,j} | y_j^n, m_1) \geq I(u_j; z_j) - I(u_j; y_j) - \varepsilon. \quad (45)$$

and therefore using the fact that $u_j \rightarrow z_j \rightarrow y_j$, we have

$$\frac{1}{n} \sum_{j=1}^L H(\bar{m}_{2,j} | y_j^n, m_1) \geq \sum_{j=1}^L I(u_j; z_j | y_j) - L\varepsilon. \quad (46)$$

We next upper bound the second term in (44). Note that

$$H(\bar{m}_{2,1}^M | m_2, m_1, y_1^n, \dots, y_M^n) \leq H(\bar{m}_{2,1}^M | m_2, m_1, y_1^n, \dots, y_L^n, z_{L+1}^n, \dots, z_M^n) \quad (47)$$

since z_j^n is a degraded version of y_j^n on channels $j \in \{L+1, \dots, M\}$. Also note that

$$\tilde{R} = \frac{1}{n}H(\bar{m}_{2,1}, \dots, \bar{m}_{2,M}) \quad (48)$$

$$= \frac{1}{n} \sum_{i=1}^M H(\bar{m}_{2,i}) \quad (49)$$

$$= \sum_{i=1}^M \{I(u_i; z_i) - 2\varepsilon\}, \quad (50)$$

where we use the fact that the messages $(\bar{m}_{2,1}, \dots, \bar{m}_{2,M})$ are mutually independent (c.f. (25)). Furthermore we select

$$R_2 = \frac{1}{n} H(m_2) \quad (51)$$

$$\leq \sum_{i=1}^L I(u_i; z_i | y_i) - (2M + 1)\varepsilon. \quad (52)$$

Note that

$$\tilde{R} - R_2 > \sum_{i=1}^L I(u_i; y_i) + \sum_{i=L+1}^M I(u_i; z_i) \quad (53)$$

$$= I(u_1, \dots, u_M; y_1, \dots, y_L, z_{L+1}, \dots, z_M) \quad (54)$$

where the last step follows from the fact that we have selected u_1, \dots, u_M to be mutually independent and the channels are also independent. We can therefore conclude that (c.f. [18, Lemma 22.1, Remark 22.2, pp. 554-555], [19, Lemma 1])

$$\begin{aligned} & \frac{1}{n} H(\bar{m}_{2,1}^M | m_2, m_1, y_1^n, \dots, y_L^n, z_{L+1}^n, \dots, z_M^n) \\ & \leq \tilde{R} - R_2 - I(u_1, \dots, u_M; y_1, \dots, y_L, z_{L+1}, \dots, z_M) + \varepsilon \end{aligned} \quad (55)$$

$$= \sum_{i=1}^L I(u_i; z_i | y_i) - R_2 + \varepsilon. \quad (56)$$

Substituting (46) and (56) into (44) we have that

$$\frac{1}{n} H(m_2 | \mathbf{y}_1^n, m_1) \geq R_2 - (L + 1)\varepsilon, \quad (57)$$

Since $\varepsilon > 0$ can be arbitrarily small, this establishes the secrecy of message m_2 with respect to user 1 in group 1. The secrecy with respect to every other user can be established in a similar fashion.

Remark 1: The superposition approach uses the codewords for the group 2 user as cloud centers and the codewords of the group 1 user as satellite codewords. To justify this, note that on any given channel, say channel i , there is an ordering of receivers as in (3). Receivers $\{\pi_i(l_i + 1), \dots, \pi(K)\}$ belonging to group 1 that are weaker than the group 2 user. It can be seen that these receivers do not learn any information on channel i . Thus among all the set of *active* users on any given channel, the group 2 user is the weakest user. Therefore the associated codeword of the group 2 user constitutes the cloud center.

IV. CONVERSE

We first show that there exists a choice of auxiliary variables $u_i(j)$ that satisfy the Markov chain condition

$$u_i(j) \rightarrow x_i(j) \rightarrow y_{\pi(1),i}(j) \cdots y_{\pi(l_i),i}(j) \rightarrow z_i(j) \rightarrow y_{\pi(l_i+1),i}(j) \cdots y_{\pi(K),i}(j). \quad (58)$$

such that the rates R_1 and R_2 are upper bounded by

$$nR_1 \leq \sum_{i=1}^M \sum_{j=1}^n I(x_i(j); y_{k,i}(j) | u_i(j), z_i(j)) + 2n\varepsilon_n \quad (59)$$

$$nR_2 \leq \sum_{i=1}^M \sum_{j=1}^n I(u_i(j); z_i(j) | y_{k,i}(j)) + 2n\varepsilon_n \quad (60)$$

for each $k \in \{1, \dots, K\}$.

In particular we show that the choice of $u_i(j)$ is given by the following:

$$u_i(j) = \left\{ m_2, \bar{\mathbf{z}}_{i \setminus i}^n, \bar{\mathbf{z}}_{i,j+1}^n, \bar{\mathbf{z}}_i^{j-1} \right\} \quad (61)$$

where we introduce (c.f. (58))

$$\bar{\mathbf{z}}_i^n := (z_i^n, y_{\pi(l_i+1),i}^n, \dots, y_{\pi(K),i}^n), \quad (62)$$

$$\bar{\mathbf{z}}_{i \setminus i}^n := (\bar{\mathbf{z}}_1^n, \dots, \bar{\mathbf{z}}_{i-1}^n, \bar{\mathbf{z}}_{i+1}^n, \dots, \bar{\mathbf{z}}_M^n), \quad (63)$$

$$\bar{\mathbf{z}}_i^{j-1} := (z_i^{j-1}, y_{\pi(l_i+1),i}^{j-1}, \dots, y_{\pi(K),i}^{j-1}), \quad (64)$$

$$\bar{\mathbf{z}}_{i,j+1}^n := (z_{i,j+1}^n, y_{\pi(l_i+1),i,j+1}^n, \dots, y_{\pi(K),i,j+1}^n), \quad (65)$$

and observe our choice of $u_i(j)$ in (61) indeed satisfies (58). Note that $\bar{\mathbf{z}}_i^n$ is the collection of the Group 2 receiver's channel output as well as the output of all the receivers $\{\pi(l_i+1), \dots, \pi(K)\}$ in Group 1 that are degraded with respect to the group 2 receiver on channel i .

We begin with the secrecy constraint associated with message m_2 with respect to user k in group 1. Let us define the following:

$$\bar{\mathbf{y}}_{k,i}^n := \begin{cases} y_{k,i}^n, & x_k \rightarrow z_i \rightarrow y_{k,i} \\ z_i^n, & x_k \rightarrow y_{k,i} \rightarrow z_i, \end{cases} \quad (66)$$

$$\bar{\mathbf{y}}_k^n := (\bar{\mathbf{y}}_{k,1}^n, \dots, \bar{\mathbf{y}}_{k,M}^n), \quad \mathbf{z}^n := (z_1^n, \dots, z_M^n), \quad (67)$$

$$\bar{\mathbf{y}}_{k,i}^n := (\bar{\mathbf{y}}_{k,1}^n, \dots, \bar{\mathbf{y}}_{k,i}^n), \quad \mathbf{z}_i^n := (z_1^n, \dots, z_i^n). \quad (68)$$

Thus $\bar{\mathbf{y}}_k^n$ corresponds to a weaker receiver, whose output on channel i is degraded to z_i^n , if user k is stronger than the group 2 user on this sub-channel. Clearly we have that $\frac{1}{n}I(m_2; \bar{\mathbf{y}}_k^n) \leq \varepsilon_n$ whenever $\frac{1}{n}I(m_2; \mathbf{y}_k^n) \leq \varepsilon_n$.

We thus have

$$n(R_2 - 2\varepsilon_n) \leq I(m_2; \mathbf{z}^n) - I(m_2; \bar{\mathbf{y}}_k^n) \quad (69)$$

$$\leq I(m_2; \mathbf{z}^n | \bar{\mathbf{y}}_k^n) \quad (70)$$

$$= \sum_{i=1}^M \sum_{j=1}^n I(m_2; z_i(j) | z_i^{j-1}, \mathbf{z}_{i-1}^n, \bar{\mathbf{y}}_k^n) \quad (71)$$

$$\leq \sum_{i=1}^M \sum_{j=1}^n I(m_2, z_i^{j-1}, z_{i,j+1}^n, \mathbf{z}_{i-1}^n, \bar{\mathbf{y}}_{k \setminus i}^n, \bar{y}_{k,i}^{j-1}, \bar{y}_{k,i,j+1}^n; z_i(j) | \bar{y}_{k,i}(j)) \quad (72)$$

$$\leq \sum_{i=1}^M \sum_{j=1}^n I(m_2, \bar{\mathbf{z}}_{i \setminus i}^n, \bar{\mathbf{z}}_{i,j+1}^n, \bar{z}_i^{j-1}; z_i(j) | \bar{y}_{k,i}(j)) \quad (73)$$

$$= \sum_{i=1}^M \sum_{j=1}^n I(u_i(j); z_i(j) | \bar{y}_{k,i}(j)) \quad (74)$$

$$= \sum_{i=1}^M \sum_{j=1}^n I(u_i(j); z_i(j) | y_{k,i}(j)) \quad (75)$$

where (73) follows from the fact that

$$(\mathbf{z}_{i-1}^n, \bar{\mathbf{y}}_{k \setminus i}^n) \subseteq \bar{\mathbf{z}}_i^n, \quad (z_i^{j-1}, \bar{y}_{k,i}^{j-1}) \subseteq \bar{z}_i^{j-1}, \quad (z_{i,j+1}^n, \bar{y}_{k,i,j+1}^n) \subseteq \bar{\mathbf{z}}_{i,j+1}^n, \quad (76)$$

and (75) follows from the fact whenever $y_{k,i}(j) \neq \bar{y}_{k,i}(j)$ then $z_i(j)$ is a degraded version of $y_{k,i}(j)$ and from (66), we have that

$$I(u_i(j); z_i(j) | y_{k,i}(j)) = I(u_i(j); z_i(j) | \bar{y}_{k,i}(j)) = 0. \quad (77)$$

This establishes (60).

Next, we upper bound R_1 as follows:

$$n(R_1 - 2\varepsilon_n) \leq I(m_1; \mathbf{y}_k^n) - I(m_1; \mathbf{z}^n, m_2) \quad (78)$$

$$\leq I(m_1; \mathbf{y}_k^n | \mathbf{z}^n, m_2) \quad (79)$$

$$\leq \sum_{i=1}^M \sum_{j=1}^n I(m_1; y_{k,i}(j) | y_{k,i}^{j-1}, \mathbf{y}_{k,i-1}^n, \mathbf{z}^n, m_2) \quad (80)$$

$$\leq \sum_{i=1}^M \sum_{j=1}^n H(y_{k,i}(j) | y_{k,i}^{j-1}, \mathbf{y}_{k,i-1}^n, \mathbf{z}^n, m_2) - H(y_{k,i}(j) | y_{k,i}^{j-1}, \mathbf{y}_{k,i-1}^n, \mathbf{z}^n, m_1, m_2, x_i(j)) \quad (81)$$

$$= \sum_{i=1}^M \sum_{j=1}^n H(y_{k,i}(j) | y_{k,i}^{j-1}, \mathbf{y}_{k,i-1}^n, \mathbf{z}^n, m_2) - H(y_{k,i}(j) | x_i(j), z_i(j)) \quad (82)$$

$$\leq \sum_{i=1}^M \sum_{j=1}^n H(y_{k,i}(j) | \mathbf{z}^n, m_2) - H(y_{k,i}(j) | x_i(j), z_i(j)) \quad (83)$$

$$= \sum_{i=1}^M \sum_{j=1}^n H(y_{k,i}(j) | \bar{\mathbf{z}}_{i \setminus i}^n, \bar{z}_i^{j-1}, \bar{\mathbf{z}}_{i,j+1}^n, z_i(j), m_2) - H(y_{k,i}(j) | x_i(j), z_i(j)) \quad (84)$$

$$= \sum_{i=1}^M \sum_{j=1}^n H(y_{k,i}(j) | u_i(j), z_i(j)) - H(y_{k,i}(j) | x_i(j), z_i(j), u_i(j)) \quad (85)$$

$$= \sum_{i=1}^M \sum_{j=1}^n I(x_i(j); y_{k,i}(j) | u_i(j), z_i(j)), \quad (86)$$

where (82) follows from the fact that for our channel model $(y_{k,i}(j), z_i(j))$ are independent of all other random variables given $x_i(j)$ whereas (84) follows from the fact that even though $\mathbf{z}^n \subseteq \{\bar{\mathbf{Z}}_{\setminus i}^n, \bar{\mathbf{z}}_i^{j-1}, \bar{\mathbf{z}}_{i,j+1}^n, z_i(j)\}$ holds, the additional elements in the latter are only a degraded version of \mathbf{z}^n . This establishes (59).

To complete the converse, let q_i to be a random variable uniformly distributed over the set $\{1, 2, \dots, n\}$ and furthermore we let $u_i = (u_i(q_i), q_i)$, $x_i = x_i(q_i)$ etc. Then (59) and (60) can be reduced to

$$R_1 - 2\varepsilon_n \leq \sum_{i=1}^M I(x_i; y_{k,i} | u_i, z_i, q_i) = \sum_{i=1}^M I(x_i; y_{k,i} | u_i, z_i) \quad (87)$$

$$R_2 - 2\varepsilon_n \leq \sum_{i=1}^M I(u_i; z_i | y_{k,i}, q_i) \leq \sum_{i=1}^M I(u_i; z_i | y_{k,i}). \quad (88)$$

The upper bound on the cardinality of \mathcal{U}_i follows by a straightforward application of Caratheodory's theorem and the proof is omitted.

A. Special case of $K = 2$ receivers

For the case when there are $K = 2$ receivers, the upper bound can be obtained via an alternative approach which involves first obtaining single-letter bounds for a particular genie-aided channel and then combining these bounds in a suitable manner.

In particular, suppose that we only need to transmit message m_1 to receiver 1 in group 1 and that the message m_2 only needs to be secure from user 2 in group 1. Under these relaxed constraints, it can be shown that any achievable rate pair (R_1, R_2) must satisfy:

$$R_1 \leq \sum_{i=1}^M I(x_i; y_{1,i} | z_i, u_i), \quad R_2 \leq \sum_{i=1}^M I(u_i; z_i | y_{2,i}), \quad (89)$$

for some auxiliary variables $\{u_i\}_{1 \leq i \leq M}$ that satisfy the Markov chain in (58). Similarly if we instead consider transmitting message m_1 only to user 2 in group 1 and require secrecy of m_2 only with respect to user 1 in group 1, it can be shown that any achievable rate pair (R_1, R_2) must satisfy:

$$R_1 \leq \sum_{i=1}^M I(x_i; y_{2,i} | z_i, v_i), \quad R_2 \leq \sum_{i=1}^M I(v_i; z_i | y_{1,i}). \quad (90)$$

for some auxiliary variables $\{v_i\}_{1 \leq i \leq M}$. Next, we show that on each sub-channel i we can always set $u_i = v_i$ without affecting the upper bound. In particular we consider the following four cases:

- Group 2 receiver satisfies $x_i \rightarrow z_i \rightarrow (y_{1,i}, y_{2,i})$: It suffices to take $u_i = v_i = x_i$ in (89) and (90) as the contribution of this sub-channel in the expressions for R_1 is always zero.
- Group 2 receiver satisfies $x_i \rightarrow (y_{1,i}, y_{2,i}) \rightarrow z_i$: It suffices to take $u_i = v_i = 0$ since the contribution of this sub-channel in the expressions for R_2 is zero.

- Group 2 receiver satisfies $x_i \rightarrow y_{1,i} \rightarrow z_i \rightarrow y_{2,i}$: Since the contribution of sub-channel i in the expressions of both R_1 and R_2 in (90) is zero, we can set $v_i = u_i$ without affecting the upper bound.
- Group 2 receiver satisfies $x_i \rightarrow y_{2,i} \rightarrow z_i \rightarrow y_{1,i}$: Since the contribution of sub-channel i in the expressions of both R_1 and R_2 in (89) is zero, we can set $u_i = v_i$ without affecting the upper bound.

Thus we need no more than one non-trivial auxiliary variable on each sub-channel. Setting $v_i = u_i$ in (90) we have

$$R_1 \leq \sum_{i=1}^M I(x_i; y_{2,i} | z_i, u_i), \quad R_2 \leq \sum_{i=1}^M I(u_i; z_i | y_{1,i}). \quad (91)$$

The converse follows by combining (89) and (91).

Unfortunately when there are more than two receivers in group 1, we have not been able to obtain the converse directly from such single-letter expressions. Therefore our approach in the previous section was to identify a single auxiliary random variable u_i as in (61) that is simultaneously compatible with all the n -letter upper bound expressions.

V. GAUSSIAN CHANNELS

In this section we provide a proof for Theorem 2. Note that the achievability of the rate pairs (R_1, R_2) constrained by (12) and (13) follows that of those constrained by (6) and (7) by setting $x_i = u_i + v_i$, where u_i and v_i are independent $\mathcal{N}(0, P_i - Q_i)$ and $\mathcal{N}(0, Q_i)$ respectively for some $0 \leq Q_i \leq P_i$ and $i = 1, \dots, M$. For the rest of the section, we shall focus on proving the converse result.

Considering proof by contradiction, let us assume that (R_1^o, R_2^o) is an achievable rate pair that lies *outside* the rate region constrained by (12) and (13). Note that the maximum rate for message m_1 is given by the right-hand side of (12) by setting $Q_i = P_i$ for all $i = 1, \dots, M$ [4], and the maximum rate for message m_2 is given by the right-hand side of (13) by setting $Q_i = 0$ for all $i = 1, \dots, M$ [1], [7]. Thus, without loss of generality we may assume that $R_2^o = R_2^* + \delta$ for some $\delta > 0$ where R_2^* is given by

$$\begin{aligned} & \max_{(\mathbf{Q}, R_2)} R_2 \\ \text{subject to } & R_1^o \leq \sum_{i=1}^M A_{k,i}^{(1)}(\mathbf{Q}), \quad \forall k = 1, \dots, K \end{aligned} \quad (92)$$

$$R_2 \leq \sum_{i=1}^M A_{k,i}^{(2)}(\mathbf{Q}), \quad \forall k = 1, \dots, K \quad (93)$$

$$Q_i \geq 0, \quad \forall i = 1, \dots, M \quad (94)$$

$$Q_i \leq P_i, \quad \forall i = 1, \dots, M. \quad (95)$$

For each $k = 1, \dots, K$ and $i = 1, \dots, M$ let α_k , β_k , $M_{1,i}$ and $M_{2,i}$ be the Lagrangians that correspond to the

constrains (92)–(95) respectively, and let

$$L := R_2 + \sum_{k=1}^K \alpha_k \left[\sum_{i=1}^M A_{k,i}^{(1)}(\mathbf{Q}) - R_1^o \right] + \sum_{k=1}^K \beta_k \left[\sum_{i=1}^M A_{k,i}^{(2)}(\mathbf{Q}) - R_2 \right] + \sum_{i=1}^M M_{1,i} Q_i + \sum_{i=1}^M M_{2,i} (P_i - Q_i). \quad (96)$$

It is straightforward to verify that the above optimization program that determines R_2^* is a convex program. Therefore, taking partial derivatives of L over Q_i , $i = 1 \dots, M$ and R_2 respectively gives the following set of Karush-Kuhn-Tucker (KKT) conditions, which must be satisfied by any *optimal* solution (\mathbf{Q}^*, R_2^*) :

$$\sum_{k \in \mathcal{Y}_i} \alpha_k (Q_i^* + \sigma_{k,i}^2)^{-1} + \sum_{k \in \mathcal{Z}_i} \beta_k (Q_i^* + \sigma_{k,i}^2)^{-1} + M_{1,i} = \left(\sum_{k \in \mathcal{Y}_i} \alpha_k + \sum_{k \in \mathcal{Z}_i} \beta_k \right) (Q_i^* + \delta_i^2)^{-1} + M_{2,i} \quad (97)$$

$$\sum_{k=1}^K \beta_k = 1 \quad (98)$$

$$\alpha_k \left[\sum_{i=1}^M A_{k,i}^{(1)}(\mathbf{Q}^*) - R_1^o \right] = 0, \quad \forall k = 1, \dots, K \quad (99)$$

$$\beta_k \left[\sum_{i=1}^M A_{k,i}^{(2)}(\mathbf{Q}^*) - R_2^* \right] = 0, \quad \forall k = 1, \dots, K \quad (100)$$

$$M_{1,i} Q_i^* = 0, \quad \forall i = 1, \dots, M \quad (101)$$

$$M_{2,i} (P_i - Q_i^*) = 0, \quad \forall i = 1, \dots, M \quad (102)$$

$$\alpha_k, \beta_k \geq 0, \quad \forall k = 1, \dots, K \quad (103)$$

$$M_{1,i}, M_{2,i} \geq 0, \quad \forall i = 1, \dots, M \quad (104)$$

where

$$\mathcal{Y}_i := \{k : \sigma_{k,i}^2 < \delta_i^2\} \quad \text{and} \quad \mathcal{Z}_i := \{k : \sigma_{k,i}^2 > \delta_i^2\}. \quad (105)$$

Note that $\delta > 0$, so we have

$$\left(\sum_{k=1}^K \alpha_k \right) R_1^o + R_2^o > \left(\sum_{k=1}^K \alpha_k \right) R_1^o + R_2^* \quad (106)$$

$$= \sum_{k=1}^K (\alpha_k R_1^o + \beta_k R_2^*) \quad (107)$$

$$= \sum_{k=1}^K \left[\alpha_k \sum_{i=1}^M A_{k,i}^{(1)}(\mathbf{Q}^*) + \beta_k \sum_{i=1}^M A_{k,i}^{(2)}(\mathbf{Q}^*) \right] \quad (108)$$

$$= \sum_{i=1}^M \sum_{k=1}^K \left[\alpha_k A_{k,i}^{(1)}(\mathbf{Q}^*) + \beta_k A_{k,i}^{(2)}(\mathbf{Q}^*) \right], \quad (109)$$

where (107) follows from the KKT condition (98), and (108) follows from the KKT conditions (99) and (100).

Next, we shall show that by assumption (R_1^o, R_2^o) is achievable, so we have

$$\left(\sum_{k=1}^K \alpha_k \right) R_1^o + R_2^o \leq \sum_{i=1}^M \sum_{k=1}^K \left[\alpha_k A_{k,i}^{(1)}(\mathbf{Q}^*) + \beta_k A_{k,i}^{(2)}(\mathbf{Q}^*) \right] \quad (110)$$

which is an apparent contradiction to (109) and hence will help to complete the proof of the theorem.

To prove (110), let us apply the converse part of Theorem 1 on (R_1^o, R_2^o) and write

$$\left(\sum_{k=1}^K \alpha_k \right) R_1^o + R_2^o \leq \left(\sum_{k=1}^K \alpha_k \right) \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^M I(x_i; y_{k,i} | u_i, z_i) \right\} + \min_{1 \leq k \leq K} \left\{ \sum_{i=1}^M I(u_i; z_i | y_{k,i}) \right\} \quad (111)$$

$$\leq \sum_{k=1}^K \left[\alpha_k \sum_{i=1}^M I(x_i; y_{k,i} | u_i, z_i) \right] + \sum_{k=1}^K \left[\beta_k \sum_{i=1}^M I(u_i; z_i | y_{k,i}) \right] \quad (112)$$

$$= \sum_{i=1}^M \sum_{k=1}^K [\alpha_k I(x_i; y_{k,i} | u_i, z_i) + \beta_k I(u_i; z_i | y_{k,i})], \quad (113)$$

where (112) follows from the well-known fact that minimum is no more than any weighted mean. By the degradedness assumption (3), we have

$$I(x_i; y_{k,i} | u_i, z_i) = I(x_i; y_{k,i} | u_i) - I(x_i; z_i | u_i) \quad (114)$$

$$= h(y_{k,i} | u_i) - h(z_i | u_i) - h(n_{k,i}) + h(w_i) \quad (115)$$

$$= h(y_{k,i} | u_i) - h(z_i | u_i) - \frac{1}{2} \log \left(\frac{\sigma_{k,i}^2}{\delta_i^2} \right) \quad (116)$$

for any $k \in \mathcal{Y}_i$ and $I(x_i; y_{k,i} | u_i, z_i) = 0$ for any $k \notin \mathcal{Y}_i$. Similarly,

$$I(u_i; z_i | y_{k,i}) = I(u_i; z_i) - (u_i; y_{k,i}) \quad (117)$$

$$= h(z_i) - h(y_{k,i}) - h(z_i | u_i) + h(y_{k,i} | u_i) \quad (118)$$

$$\leq \frac{1}{2} \log \left(\frac{P_i + \delta_i^2}{P_i + \sigma_{k,i}^2} \right) - h(z_i | u_i) + h(y_{k,i} | u_i) \quad (119)$$

for any $k \in \mathcal{Z}_i$, where (119) follows from the worst additive noise Lemma [20], and $I(u_i; z_i | y_{k,i}) = 0$ for any $k \notin \mathcal{Z}_i$. Thus, for each $i = 1, \dots, M$ we have

$$\begin{aligned} & \sum_{k=1}^K [\alpha_k I(x_i; y_{k,i} | u_i, z_i) + \beta_k I(u_i; z_i | y_{k,i})] \\ & \leq \sum_{k \in \mathcal{Y}_i} \alpha_k \left[h(y_{k,i} | u_i) - h(z_i | u_i) - \frac{1}{2} \log \left(\frac{\sigma_{k,i}^2}{\delta_i^2} \right) \right] + \\ & \quad \sum_{k \in \mathcal{Z}_i} \beta_k \left[\frac{1}{2} \log \left(\frac{P_i + \delta_i^2}{P_i + \sigma_{k,i}^2} \right) - h(z_i | u_i) + h(y_{k,i} | u_i) \right] \end{aligned} \quad (120)$$

$$\begin{aligned} & = \sum_{k \in \mathcal{Y}_i} \alpha_k h(y_{k,i} | u_i) + \sum_{k \in \mathcal{Z}_i} \beta_k h(y_{k,i} | u_i) - \left(\sum_{k \in \mathcal{Y}_i} \alpha_k + \sum_{k \in \mathcal{Z}_i} \beta_k \right) h(z_i | u_i) - \\ & \quad \sum_{k \in \mathcal{Y}_i} \frac{\alpha_k}{2} \log \left(\frac{\sigma_{k,i}^2}{\delta_i^2} \right) + \sum_{k \in \mathcal{Z}_i} \frac{\beta_k}{2} \log \left(\frac{P_i + \delta_i^2}{P_i + \sigma_{k,i}^2} \right). \end{aligned} \quad (121)$$

We have the following lemma, which is the scalar version of the extremal inequality established in [17, Theorem 2].

Lemma 2: For any real scalars α_k , β_k , Q_i^* , $M_{1,i}$ and $M_{2,i}$ that satisfy KKT conditions (97) and (101)–(104), we have

$$\begin{aligned} & \sum_{k \in \mathcal{Y}_i} \alpha_k h(y_{k,i}|u_i) + \sum_{k \in \mathcal{Z}_i} \beta_k h(y_{k,i}|u_i) - \left(\sum_{k \in \mathcal{Y}_i} \alpha_k + \sum_{k \in \mathcal{Z}_i} \beta_k \right) h(z_i|u_i) \\ & \leq \sum_{k \in \mathcal{Y}_i} \frac{\alpha_k}{2} \log(Q_i^* + \sigma_{k,i}^2) + \sum_{k \in \mathcal{Z}_i} \frac{\beta_k}{2} \log(Q_i^* + \sigma_{k,i}^2) - \frac{\sum_{k \in \mathcal{Y}_i} \alpha_k + \sum_{k \in \mathcal{Z}_i} \beta_k}{2} \log(Q_i^* + \delta_i^2) \end{aligned} \quad (122)$$

for any (u_i, x_i) that is independent of the additive Gaussian noise $(n_{1,i}, \dots, n_{K,i}, w_i)$ and such that $E[x_i^2] \leq P_i$.

□

We note here that the extremal inequality in [17, Theorem 2] was established using a *vector* generalization of Costa's entropy-power inequality. The scalar version that we used here, however, can be directly established using the *original* Costa's entropy-power inequality [16]. Substituting (122) into (121) gives

$$\begin{aligned} & \sum_{k=1}^K [\alpha_k I(x_i; y_{k,i}|u_i, z_i) + \beta_k I(u_i; z_i|y_{k,i})] \\ & \leq \sum_{k \in \mathcal{Y}_i} \frac{\alpha_k}{2} \log(Q_i^* + \sigma_{k,i}^2) + \sum_{k \in \mathcal{Z}_i} \frac{\beta_k}{2} \log(Q_i^* + \sigma_{k,i}^2) - \frac{\sum_{k \in \mathcal{Y}_i} \alpha_k + \sum_{k \in \mathcal{Z}_i} \beta_k}{2} \log(Q_i^* + \delta_i^2) - \\ & \quad \sum_{k \in \mathcal{Y}_i} \frac{\alpha_k}{2} \log\left(\frac{\sigma_{k,i}^2}{\delta_i^2}\right) + \sum_{k \in \mathcal{Z}_i} \frac{\beta_k}{2} \log\left(\frac{P_i + \delta_i^2}{P_i + \sigma_{k,i}^2}\right) \end{aligned} \quad (123)$$

$$\begin{aligned} & = \sum_{k \in \mathcal{Y}_i} \alpha_k \left[\frac{1}{2} \log\left(\frac{Q_i^* + \sigma_{k,i}^2}{\sigma_{k,i}^2}\right) - \frac{1}{2} \log\left(\frac{Q_i^* + \delta_i^2}{\delta_i^2}\right) \right] + \\ & \quad \sum_{k \in \mathcal{Z}_i} \beta_k \left[\frac{1}{2} \log\left(\frac{P_i + \delta_i^2}{Q_i^* + \delta_i^2}\right) - \frac{1}{2} \log\left(\frac{P_i + \sigma_{k,i}^2}{Q_i^* + \sigma_{k,i}^2}\right) \right] \end{aligned} \quad (124)$$

$$= \sum_{k=1}^K \left[\alpha_k A_{k,i}^{(1)}(\mathbf{Q}^*) + \beta_k A_{k,i}^{(2)}(\mathbf{Q}^*) \right]. \quad (125)$$

Further substituting (125) into (113) completes the proof of (110). We have thus completed the proof of Theorem 2.

VI. FADING CHANNELS

To establish the connection to fading channels, first observe that Theorem 2 and Corollary 1 can be extended in the following way. Consider the following scalar Gaussian broadcast channel with $K + 1$ users:

$$y_k(t) = x(t) + n_k(t) \quad (126)$$

$$z(t) = x(t) + w(t), \quad t = 1, \dots, T. \quad (127)$$

At each time sample t , the additive noise $(n_1(t), \dots, n_K(t), w(t))$ are independent zero-mean Gaussian with the variances $(\sigma_1^2, \dots, \sigma_K^2, \delta^2)$ selected at random as $(\sigma_{1,i}^2, \dots, \sigma_{K,i}^2, \delta_i^2)$ with probability p_i , $i = 1, \dots, M$. Both the selection of the noise variances and the realization of the additive noise are assumed to be independent across the time index t and revealed to all the terminals. We are interested in the ergodic scenario where the duration T of communication can be arbitrarily large. The following extension of Theorem 2 readily follows and its proof will be omitted.

Corollary 2: For the scalar Gaussian broadcast channel considered above, the capacity region consists of all rate pairs (R_1, R_2) that satisfy

$$R_1 \leq \min_{1 \leq k \leq K} \sum_{i=1}^M p_i \left[\frac{1}{2} \log \left(\frac{Q_i + \sigma_{k,i}^2}{\sigma_{k,i}^2} \right) - \frac{1}{2} \log \left(\frac{Q_i + \delta_i^2}{\delta_i^2} \right) \right]^+ \quad (128)$$

$$R_2 \leq \min_{1 \leq k \leq K} \sum_{i=1}^M p_i \left[\frac{1}{2} \log \left(\frac{P_i + \delta_i^2}{Q_i + \delta_i^2} \right) - \frac{1}{2} \log \left(\frac{P_i + \sigma_{k,i}^2}{Q_i + \sigma_{k,i}^2} \right) \right]^+ \quad (129)$$

for some $0 \leq Q_i \leq P_i$ and $i = 1, \dots, M$. \square

Clearly if the fading coefficients in (17) are all discrete-valued, then the result in Theorem 3 follows immediately from Corollary 2. When the fading coefficients are continuous valued, we can generalize Theorem 2 by suitably quantizing the channel gains.

First without loss of generality, we assume that each fading coefficient is real-valued, since each receiver can cancel out the phase of the fading gain through a suitable multiplication at the receiver. Consider a discrete set

$$\mathcal{A} := \{A_1, A_2, \dots, A_N, A_{N+1}\}$$

where $A_i \leq A_{i+1}$, $A_1 := 0$, $A_N := J$ and $A_{N+1} := \infty$ holds.

Given a set of channel gains $(h_1(i), \dots, h_K(i), g(i))$ in coherence block i , we discretize them to one of $(N+1)^{K+1}$ states as described below.

- Encoding message m_1 : Suppose that the channel gain of receiver k satisfies $A_q \leq h_k(i) \leq A_{q+1}$, then we assume that the channel gain equals $s_{i,k} = A_q$. If the channel gain of the group 2 user satisfies $A_q \leq g(i) \leq A_{q+1}$ then we assume that its channel gain equals $\bar{s}_{i,K+1} = A_{q+1}$.
- Encoding message m_2 : Suppose that the channel gain of the group 2 receiver satisfies $A_q \leq g(i) \leq A_{q+1}$, then we assume that the channel gain equals $s_{K+1} = A_q$. If the channel gain of a group 1 receiver satisfies $A_q \leq h_k(i) \leq A_{q+1}$ then we assume it equals $\bar{s}_k = A_{q+1}$.

Thus the channel gains in coherence block are mapped to one of $L = (N+1)^{K+1}$ states $\{\mathbf{s}_j\}_{j=1}^L$. We denote the channel gains of the associated receivers in state \mathbf{s}_j as $(s_{j,1}, \dots, s_{j,K}, s_{j,K+1})$ and the channel gains of the associated eavesdroppers as $(\bar{s}_{j,1}, \dots, \bar{s}_{j,K+1})$. Note that in our notation, the K receivers in group 1 are labeled $\{1, \dots, K\}$ while the group 2 receiver is labeled $\{K+1\}$.

With the above quantization procedure it suffices to consider a coding scheme associated for $L = (N+1)^{K+1}$ parallel channels, where each parallel channel corresponds to one state realization \mathbf{s}_j . Using Corollary 2 the

following rate pair (R_1, R_2) is achievable:

$$R_1 \leq \min_{1 \leq k \leq K} \sum_{j=1}^L \Pr(\mathbf{s}_j) A_{j,k}^{(1)}(\mathbf{s}_j) \quad (130)$$

$$R_2 \leq \min_{1 \leq k \leq K} \sum_{j=1}^L \Pr(\mathbf{s}_j) A_{j,k}^{(2)}(\mathbf{s}_j), \quad (131)$$

where

$$A_{j,k}^{(1)}(\mathbf{s}_j) := \left\{ \log \frac{1 + Q(\mathbf{s}_j)|s_{j,k}|^2}{1 + Q(\mathbf{s}_j)|\bar{s}_{j,K+1}|^2} \right\}^+ \quad (132)$$

$$A_{j,k}^{(2)}(\mathbf{s}_j) := \left\{ \log \frac{1 + P(\mathbf{s}_j)|s_{j,K+1}|^2}{1 + Q(\mathbf{s}_j)|s_{j,K+1}|^2} - \log \frac{1 + P(\mathbf{s}_j)|\bar{s}_{j,k}|^2}{1 + Q(\mathbf{s}_j)|\bar{s}_{j,k}|^2} \right\}^+. \quad (133)$$

For any J , taking the limit $N \rightarrow \infty$ we have that

$$\sum_{j=1}^L \Pr(\mathbf{s}_j) A_{j,k}^{(1)}(\mathbf{h}, g) \rightarrow \oint_0^J \int_0^J A_k^{(1)}(\mathbf{h}, g) dF(g) dF(\mathbf{h}) \quad (134)$$

$$= \oint_0^J \int_0^\infty A_k^{(1)}(\mathbf{h}, g) dF(g) dF(\mathbf{h}) \quad (135)$$

where

$$A_k^{(1)}(\mathbf{h}, g) = \left\{ \log \frac{1 + Q(\mathbf{h}, g)|h_k|^2}{1 + Q(\mathbf{h}, g)|g|^2} \right\}^+,$$

and (135) follows from the fact that $A_k^{(1)}(\cdot) = 0$ for $\bar{s}_{K+1} > J$. Finally, by taking J arbitrarily large, the right hand side in (130) approaches

$$R_1 \leq \min_{1 \leq k \leq K} \oint_0^\infty \int_0^\infty A_k^{(1)}(\mathbf{h}, g) dF(g) dF(\mathbf{h}) \quad (136)$$

as required. In a similar fashion the achievability of R_2 can be established.

The converse follows by noticing that if the channel gains are revealed non-causally to the terminals, the system reduces to a parallel channel model and the result in Theorem 2 immediately applies.

A. Numerical Results

In order to evaluate the achievable rate region, we assume that the fading gains are all sampled from $\mathcal{CN}(0, 1)$. Furthermore instead of finding the optimal power allocation we assume a potentially sub-optimal power allocation:

$$Q(\mathbf{h}, g) = \begin{cases} P, & |g|^2 \geq \theta \\ 0, & |g|^2 < \theta. \end{cases} \quad (137)$$

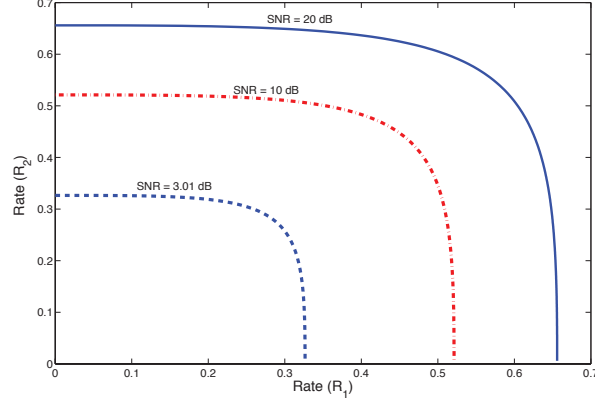


Fig. 2: Achievable rates (nats/symbol) for the two groups at different SNR values. The x-axis shows the rate R_1 for group 1 whereas the y-axis shows the rate R_2 for group 2.

where θ is a certain fixed parameter and assume that $P(\mathbf{h}, g) = P$ for all values of (\mathbf{h}, g) . Notice that our power allocation does not depend on the channel gains of the receivers in group 1. This is a reasonable simplification when K is large and the channel gains (h_1, \dots, h_K) are identically distributed. The achievable rate expressions (19) and (20) reduce to:

$$R_1 \leq \Pr(|g|^2 \leq \theta) E \left[\left\{ \log \frac{1 + P|h|^2}{1 + P|g|^2} \right\}^+ \middle| |g|^2 \leq \theta \right] \quad (138)$$

$$R_2 \leq \Pr(|g|^2 \geq \theta) E \left[\left\{ \log \frac{1 + P|g|^2}{1 + P|h|^2} \right\}^+ \middle| |g|^2 \geq \theta \right] \quad (139)$$

In Fig. 2, we plot the achievable rates for $P \in \{2, 10, 100\}$. We make the following observations:

- The corner points for R_1 and R_2 are obtained by setting $\theta = \infty$ and $\theta = 0$ respectively. By symmetry of the rate expressions in (138) and (139), it is clear that both the corner points evaluate to the same numerical constant.
- As we approach the corner point $(0, R_2)$ the boundary of the capacity region is nearly flat. Any coherence block, where $|g(i)| \leq \min_{1 \leq k \leq K} |h_k(i)|$ is clearly not useful to the group 2 receiver. By transmitting m_1 in these slots one can increase the rate R_1 without decreasing R_2 .
- As we approach the corner point $(R_1, 0)$, the boundary of the capacity region is nearly vertical. The argument is very similar to the previous case. In any period where $|g(i)| \geq \max_{1 \leq k \leq K} |h_k(i)|$ one cannot transmit to group 1. By transmitting m_2 in these slots we increase R_2 without decreasing R_1 .
- We observe that a natural alternative to the proposed scheme is time-sharing. The rate achieved by such a scheme corresponds to a straight line connecting the corner points. The rate-loss associated with such a

scheme is significant compared to the proposed scheme.

VII. CONCLUSIONS

We establish the optimality of a superposition construction for private broadcasting of two messages to two groups of receivers over independent parallel channels, when there are an arbitrary number of receivers in group 1 but there is only one receiver in group 2. We observe that in the optimal construction the codewords of group 2 must constitute the “cloud centers” whereas the codewords of group 1 must constitute the “satellite codewords”. For the case of Gaussian sub-channels the optimality of Gaussian codebooks is established. This is accomplished by obtaining a Lagrangian dual for each point on the boundary of the capacity region and then using an extremal inequality to show that the resulting expression is maximized using a Gaussian input distribution. An extension to block-fading channels is also discussed. Numerical results for Rayleigh-fading channels indicate that the proposed scheme can provide significant performance gains over naive time-sharing techniques.

REFERENCES

- [1] P. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [2] Z. Li, R. D. Yates, and W. Trappe, “Achieving Secret Communication for Fast Rayleigh Fading Channels,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 9, pp. 2792–2799, 2010.
- [3] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.
- [4] A. Khisti, A. Tchamkerten, and G. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2453–2469, 2008.
- [5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.
- [6] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wiretap channels,” *EURASIP Journal on Wireless Communications and Networking - Special issue on wireless physical layer security*, Mar. 2009.
- [7] T. Liu, V. Prabhakaran, and S. Vishwanath, “The secrecy capacity of a class of parallel gaussian compound wiretap channels,” in *Proc. Int. Symp. Inform. Theory*, 2008, pp. 116–120.
- [8] N. Cai and K. Y. Lam, “How to broadcast privacy: Secret coding for deterministic broadcast channels,” *Numbers, Information, and Complexity (Festschrift for Rudolf Ahlswede)*, eds: I. Althofer, N. Cai, G. Dueck, L. Khachatrian, M. Pinsker, A. Sarkozy, I. Wegener, and Z. Zhang, pp. 353–368, 2000.
- [9] R. Liu, T. Liu, H. Poor, and S. Shamai, “Multiple-input multiple-output gaussian broadcast channels with confidential messages,” *IEEE Trans. Inform. Theory*, no. 9, pp. 4215 – 4227, 2010.
- [10] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions,” *IEEE Trans. Inform. Theory*, June 2008.
- [11] L. Czap, V. M. Prabhakaran, S. N. Diggavi, and C. Fragouli, “Broadcasting private messages securely,” in *ISIT*, 2012, pp. 428–432.
- [12] S. Yang, P. Piantanida, M. Kobayashi, and S. Shamai, “On the secrecy degrees of freedom of multi-antenna wiretap channels with delayed CSIT,” in *ISIT*, 2011, pp. 2866–2870.
- [13] A. Khisti, “Interference alignment for the multi-antenna compound wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 57, no. 5, pp. 2967–2993, 2011.

- [14] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, 1978.
- [15] A. A. El Gamal, "Capacity of the product and sum of two un-matched broadcast channels," *Probl. Inform. Transmission*, pp. 3–23, 1980.
- [16] M. H. M. Costa, "A new entropy power inequality," *IEEE Trans. Inform. Theory*, vol. 31, no. 6, pp. 751–760, 1985.
- [17] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "A vector generalization of costa's entropy-power inequality with applications," *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1865–1879, 2010.
- [18] A. E. Gamal and Y. H. Kim, *Network Information Theory*. Cambridge, UK: Cambridge University Press, 2011.
- [19] Y. Chia and A. E. Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 2748–2765, 2012.
- [20] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inform. Theory*, vol. IT-47, no. 7, pp. 3072–3081, 2001.